ACTA ARITHMETICA
107.1 (2003)

On the relative class number of cyclotomic function fields

by

Hwanyup Jung and Jaehyun Ahn (Daejon)

1. Introduction. In cyclotomic theory over $\mathbb{Q}$, ideal class groups and class numbers of $\mathbb{Q}(\zeta_{p^n})$ and its maximal real subfield $\mathbb{Q}(\zeta_{p^n})^+$ are important objects; especially, there are many results on the relative class group and the relative class number. In [Ha], Hazama expressed the relative class number as the determinant of the Dem'yanenko matrix up to a simple factor. It was pointed out by Reyssat that the Dem'yanenko matrix is also related to the signatures of the cyclotomic units. Putting these together, Schwarz [S] obtained results on the parity of h_p^-, an immediate corollary being the well-known result that if h_p^+ is even then h_p^- is even. In [J], Jha found bases of the Stickelberger ideal I and its minus part I^-. Let R be the integral group ring of the Galois group. From the group structure of R^-/I^-, he also obtained some result on the exponent of the relative ideal class group.

Let $\mathbb{A} = \mathbb{F}_q[T]$ be the ring of polynomials over a finite field $\mathbb{F}_q$ with q elements, and $k = \mathbb{F}_q(T)$. Let ∞ be the place of k associated to $(1/T)$ and k_∞ be the completion of k at ∞. Clearly $k_\infty = \mathbb{F}_q((1/T))$. For each nonzero $M \in \mathbb{A}$, one uses the Carlitz module ϱ to construct a field extension K_M, called the Mth *cyclotomic function field*, and its maximal real subfield K_M^+. Let $G_M = \mathrm{Gal}(K_M/k)$ and $G_M^+ = \mathrm{Gal}(K_M^+/k)$. Let $\mathcal{O}_M$ and $\mathcal{O}_M^+$ be the integral closure of $\mathbb{A}$ in K_M and K_M^+, respectively. Let Cl_M and $\widetilde{Cl}_M$ be the *group of degree zero divisor classes* of K_M and the *ideal class group* of $\mathcal{O}_M$, respectively. Let $h_M = |Cl_M|$ and $\widetilde{h}_M = |\widetilde{Cl}_M|$, called the *divisor class number* and the *ideal class number* of K_M, respectively. For the maximal real subfield K_M^+, $Cl_M^+, \widetilde{Cl}_M^+, h_M^+$ and $\widetilde{h}_M^+$ are defined similarly. Let Cl_M^- and $\widetilde{Cl}_M^-$ be the minus parts of Cl_M and $\widetilde{Cl}_M$, respectively. We call them the *relative divisor class group* and *relative ideal class group* of K_M, respectively.

Let $h_M^- = |Cl_M^-|$ and $\widetilde{h}_M^- = |\widetilde{Cl}_M^-|$, called the *relative divisor class number* and *relative ideal class number* of K_M, respectively. It is known that $h_M^- =$

2000 *Mathematics Subject Classification*: 11R58, 11R60.

h_M/h_M^+ and $\widetilde{h}_M^- = \widetilde{h}_M/\widetilde{h}_M^+$. When $M = P^n$ is a prime power, it is also known [Y, Lemma 3] that $h_M^- = (q-1)^{r-1}\widetilde{h}_M^-$, where $r = q^{(n-1)\deg P}(q^{\deg P}-1)/(q-1)$. In [JA], we introduced the Dem'yanenko matrix in the function field case and expressed the relative ideal class number $\widetilde{h}_{P^n}^-$ as the determinant of this matrix.

The organization of this paper is as follows. In Section 2, we find a basis of the minus part I^- of the Stickelberger ideal I (Lemma 2.1) and its transition matrix with respect to some basis of the minus part R^- of the group ring $R = \mathbb{Z}[G]$, which is the Dem'yanenko matrix (Proposition 2.3). By an analytic method, we show that the determinant of the Dem'yanenko matrix is equal to $\widetilde{h}_{P^n}^-$ (Proposition 2.6). We also find a matrix whose determinant gives us the relative divisor class number $h_{P^n}^-$ (Proposition 2.5).

In Section 3, adopting ideas of Iwasawa [I] and Jha [J], we give some results on the exponent of the relative divisor class group $Cl_{P^n}^-$. Using the invariants of R^-/I^- and these results, we determine the group structure of the relative divisor class group $Cl_{P^n}^-$ for some special cases (Examples 1, 2).

In Section 4, we show that the sign of cyclotomic units coincides with the sign of the polynomial which acts on cyclotomic units. Using this result, we obtain a result on the 2-parity between $\widetilde{h}_{P^n}^-$ and $\widetilde{h}_{P^n}^+$ for $q = 3$ (Theorem 4.4), as an analog of Schwarz [S]. Let l be any prime divisor of $q-1$. For general q, this result should be extended on the l-parity between $\widetilde{h}_{P^n}^-$ and $\widetilde{h}_{P^n}^+$.

2. Dem'yanenko matrix and relative class number. For $M \in \mathbb{A}$, it is well known that the Galois group G_M of K_M over k is isomorphic to $(\mathbb{A}/M)^*$. Let σ_A be an element of G_M defined by $\sigma_A(\lambda) = \varrho_A(\lambda)$ for any nonzero M-torsion point λ. We write $\varrho_A(\lambda) = \lambda^A$ for simplicity. Then the isomorphism $\varphi : (\mathbb{A}/M)^* \to G_M$ is given by $\varphi(A \bmod M) = \sigma_A$. Under this isomorphism, $J = \{\sigma_\alpha : \alpha \in \mathbb{F}_q^*\}$ is the Galois group of K_M over K_M^+. For any subset H of G_M, let $s(H) = \sum_{\sigma\in H}\sigma$.

Let $\widehat{G}_M$ be the group of characters of G_M with values in $\mathbb{C}$. A character χ of G_M is called *even* if its restriction to J is trivial, and *odd* otherwise. Let $\widehat{G}_M^+ = \{\chi \in \widehat{G}_M : \chi \text{ is even}\}$ and $\widehat{G}_M^- = \widehat{G}_M \setminus \widehat{G}_M^+$. Any character χ of G_M can be viewed as a character of $(\mathbb{A}/M)^*$, so the conductor F_χ of χ is defined as a divisor of M.

For a nonzero polynomial $M \in \mathbb{A}$, we let $\mathbb{M}_M$ (resp. $\mathbb{M}_M^+$) be the set of all the polynomials (resp. monic polynomials) in $\mathbb{A}$ with degree less than the degree of M and prime to M. Let $\mathbb{M}_M^- = \mathbb{M}_M \setminus \mathbb{M}_M^+$. Fix nonzero $M \in \mathbb{A}$. For each polynomial A prime to M, we let $\overline{A} \in \mathbb{M}_M$ be the unique element such that $A \equiv \overline{A} \bmod M$. For $A \in \mathbb{A}$, we let $\operatorname{sgn}(A)$ be the leading coefficient of A and $\operatorname{sgn}_M(A) = \operatorname{sgn}(\overline{A})$ when A is prime to M. For $A \in \mathbb{M}_M$, let A' be the unique element of $\mathbb{M}_M$ such that $AA' \equiv 1 \bmod M$ and let $\widetilde{A} = A/\mathrm{sgn}_M(A) \in \mathbb{M}_M^+$.

From now on we assume $M = P^n$, a power of a monic irreducible polynomial P with $n \geq 1$. We write $K = K_M$ and $G = G_M$ for simplicity. Let $R = \mathbb{Z}[G]$, the integral group ring of G. It is well known [BK, R] that

$$h_M^- = \prod_{\chi \text{ odd}} \Big(\sum_{A \in \mathbb{M}_M^+} \chi(A) \Big). \tag{2.1}$$

Let $\theta_M = \sum_{\tau \in G_M} Z_M(0,\tau)\tau^{-1}$, where $Z_M(s,\tau)$ is the partial zeta function associated to τ. It is a Stickelberger element of the extension K/k. From [JA, (3)], we can write θ_M as follows:

$$\theta_M = \sum_{A \in \mathbb{M}_M^+} \sigma_A^{-1} - \frac{s(G)}{q-1}. \tag{2.2}$$

Let $\theta = s(G)/(q-1)$. Let S be the G-submodule of $\mathbb{Q}[G]$ generated by θ_M and θ and let $I = S \cap R$, called the *Stickelberger ideal* of K (cf. [JA, Definition 3.1]). We define $S^- = e^- S \cap S$ and $I^- = S^- \cap R = e^- I \cap I$, where $e^+ = s(J)/(q-1)$ and $e^- = 1 - e^+$. Let $\eta = \sum_{A \in \mathbb{M}_M^+} \sigma_A^{-1}$ and "deg" be the augmentation map on $\mathbb{Q}[G]$, i.e., $\deg(\sum_{\sigma \in G} a_\sigma \sigma) = \sum_{\sigma \in G} a_\sigma$ for any $\sum_{\sigma \in G} a_\sigma \sigma \in \mathbb{Q}[G]$.

LEMMA 2.1. *$\{(\sigma_A - 1)\theta_M : A \in \mathbb{M}_M^-\}$ forms a $\mathbb{Z}$-basis of I^-.*

Proof. Since $e^-\theta_M = \theta_M$ and $e^-\theta = 0$, we have $S^- = R\theta_M$ and $I^- = R\theta_M \cap R$. Let I^* be the $\mathbb{Z}$-submodule of R generated by $\{\sigma_A - 1 : A \in \mathbb{M}_M\}$. First we show that $I^- = I^*\theta_M$. Clearly $I^*\theta_M$ is contained in I^-. Let $x = \sum_{A \in \mathbb{M}_M} a_A \sigma_A \in R$ be such that $x\theta_M \in I^-$. Then $(q-1) \mid \deg x$ because

$$x\theta_M = \sum_{A \in \mathbb{M}_M} a_A(\sigma_A - 1)\theta_M + (\deg x)\theta_M.$$

So to show that $x\theta_M \in I^*\theta_M$, it suffices to show that $(q-1)\theta_M \in I^*\theta_M$. But since $s(J)\theta_M = 0$, we have $(q-1)\theta_M = \sum_{\alpha \in \mathbb{F}_q^*}(1 - \sigma_\alpha)\theta_M \in I^*\theta_M$. For any $A \in \mathbb{M}_M^+$, $s(J)(\sigma_A - 1)\theta_M = 0$. So

$$(\sigma_A - 1)\theta_M = -\sum_{1 \neq \alpha \in \mathbb{F}_q^*} ((\sigma_{\alpha A} - 1)\theta_M - (\sigma_\alpha - 1)\theta_M).$$

Thus $\{(\sigma_A - 1)\theta_M : A \in \mathbb{M}_M^-\}$ generates I^- as $\mathbb{Z}$-module. But I^- has $\mathbb{Z}$-rank $|\mathbb{M}_M^-|$ (cf. [Y, Lemma 6]). Thus it must be a $\mathbb{Z}$-basis of I^-. ∎

Next we find a $\mathbb{Z}$-basis of $R^- = R \cap e^- R$.

LEMMA 2.2. *$\{(\sigma_\alpha - 1)\sigma_A : 1 \neq \alpha \in \mathbb{F}_q^*$ and $A \in \mathbb{M}_M^+\}$ forms a $\mathbb{Z}$-basis of R^-.*

Proof. Let j be a generator of J. Then it is easy to show that $R^- = (1-j)R$. So $(\sigma_\alpha - 1)\sigma_A \in R^-$ for any $1 \neq \alpha \in \mathbb{F}_q^*$ and $A \in \mathbb{M}_M^+$. Any element of R^- can be written as a $\mathbb{Z}$-linear combination of elements of the form $(1-j)\sigma_\alpha\sigma_A$ with $\alpha \in \mathbb{F}_q^*$ and $A \in \mathbb{M}_M^+$. But

$$(1-j)\sigma_\alpha\sigma_A = (\sigma_\alpha - \sigma_{\alpha'})\sigma_A = (\sigma_\alpha - 1)\sigma_A - (\sigma_{\alpha'} - 1)\sigma_A$$

for some $\alpha' \in \mathbb{F}_q^*$. So $\{(\sigma_\alpha - 1)\sigma_A : 1 \neq \alpha \in \mathbb{F}_q^* \text{ and } A \in \mathbb{M}_M^+\}$ generates R^- as $\mathbb{Z}$-module. Since the cardinality of this set is equal to the $\mathbb{Z}$-rank of R^-, we get the result. ∎

We recall the definition of Dem'yanenko matrix in the function field case. For $A, B \in \mathbb{M}_M^-$, we let $\langle AB\rangle = 1$ if $\operatorname{sgn}_M(AB) = 1$ and $\langle AB\rangle = 0$ otherwise. Define $\mathcal{D}_M = (\langle AB\rangle)_{A,B}$, where A, B run through $\mathbb{M}_M^-$.

Proposition 2.3. $[R^- : I^-] = |\det \mathcal{D}_M|$.

Proof. Let

$$Y_1 = \{(\sigma_\alpha - 1)\sigma_A : 1 \neq \alpha \in \mathbb{F}_q^* \text{ and } A \in \mathbb{M}_M^+\},$$
$$Y_2 = \{(\sigma_A - 1)\theta_M : A \in \mathbb{M}_M^-\}.$$

Note that $(\sigma_A - 1)\theta_M = (\sigma_A - 1)(\eta - s(G)/(q-1)) = (\sigma - 1)\eta$. Thus from [JA, (5)] and the proof of [JA, Theorem 3.1], we see that the transition matrix of Y_2 with respect to Y_1 is $\mathcal{D}_M$. So we get the result. ∎

The Dem'yanenko matrix $\mathcal{D}_M$ gives the complete group structure of the quotient R^-/I^-. In Section 3, we investigate the exponent of the relative divisor class group Cl_M^- by using the quotient R^-/I^-.

The following lemma is a generalization of the Dedekind determinant formula [W, Lemma 5.26].

Lemma 2.4. *Let G be a finite abelian group and H be a subgroup of G. Let f be a function on G with values in some field of characteristic 0. Let $\mathcal{R}$ be a full set of representatives for G/H. For $\sigma \in G$, let $\overline{\sigma}$ be an element of $\mathcal{R}$ with $\sigma H = \overline{\sigma} H$. Then*

$$\prod_{\chi \in \widehat{G} \setminus \widehat{G/H}} \Big(\sum_{\sigma \in G} \chi(\sigma) f(\sigma)\Big) = \det(f(\sigma\tau^{-1}) - f(\sigma\overline{\tau}^{-1}))_{\sigma,\tau},$$

where σ, τ run through $G \setminus \mathcal{R}$.

Proof. We follow almost all the notations of the proof of [W, Lemma 5.26]. We only modify W to be the subspace of V consisting of functions $h(X)$ with $\sum_{\tau \in H} h(\sigma\tau) = 0$ for all $\sigma \in \mathcal{R}$, and for $\tau \in G$, set

$$\psi_\tau(X) = \phi_\tau(X) - \frac{1}{|H|} \sum_{\sigma \in H} \phi_{\tau\sigma}(X).$$

By comparing the transition matrices of $T = \sum_{\sigma\in G} f(\sigma)\sigma$ with respect to two bases $\{\psi_\tau(X)\}_{\tau\notin\mathcal{R}}$ and $\{\chi(X)\}_{\chi\in\widehat{G}\setminus\widehat{G/H}}$, we get the lemma. ∎

Rosen [R] obtained a determinant formula for the relative divisor class number h_P^- and his formula was extended to the prime power case by Bae–Kang [BK]. The following proposition provides us with another determinant formula for h_M^-.

PROPOSITION 2.5. $h_M^- = |\det(\langle AB'\rangle - \langle A\widetilde{B}'\rangle)_{A,B\in\mathbb{M}_M^-}|$.

Proof. From (2.1) and Lemma 2.4 with $H = J$ and $\mathcal{R} = \{\sigma_A : A \in \mathbb{M}_M^+\}$, we have

$$h_M^- = \prod_{\chi\,\mathrm{odd}} \sum_{A\in\mathbb{M}_M^+} \chi(A)\langle A\rangle = |\det(\langle AB'\rangle - \langle A\widetilde{B}'\rangle)_{A,B\in\mathbb{M}_M^-}|. \ ∎$$

PROPOSITION 2.6. $\widetilde{h}_M^- = |\det(\langle AB'\rangle)_{A,B\in\mathbb{M}_M^-}| = |\det\mathcal{D}_M|$.

Proof. Let $D = (\langle AB'\rangle - \langle A\widetilde{B}'\rangle)_{A,B\in\mathbb{M}_M^-}$ and $D_1 = (\langle AB'\rangle)_{A,B\in\mathbb{M}_M^-}$. First, we make a partition of the column indices $\mathbb{M}_M^-$ of D into r sets, say $X_1,\ldots,X_r$, such that $X_1 = \mathbb{F}_q^*\setminus\{1\}$ and if $B_1, B_2 \in X_i$, then $\widetilde{B_1} = \widetilde{B_2}$ for each i. Then $X_i = \{\alpha\widetilde{B} : 1 \neq \alpha \in \mathbb{F}_q^*\}$ for some monic $\widetilde{B} \in \mathbb{M}_M^+$. It is easy to see that the sum of columns with indices in X_i is $(1\ldots1)^{\mathrm{t}}$ for $i = 1$ and $(\ldots 1-(q-1)\langle A\widetilde{B}'\rangle\ldots)^{\mathrm{t}}_{A\in\mathbb{M}_M^-}$ for $i \neq 1$. Here B is any polynomial in X_i. Thus, by making elementary column operations on D, we find that $\det D = \pm(q-1)^{r-1}\det D_2$ where D_2 is equal to D_1 except for one column in each X_i, $i \neq 2$, and any other column in D_2 is $(\ldots\langle A\widetilde{B}'\rangle\ldots)^{\mathrm{t}}_{A\in\mathbb{M}_M^-}$ for some $B \in X_i$. Since

$$\langle A\widetilde{B}_0'\rangle + \sum_{B\in X_i}\langle AB'\rangle = 1 \tag{2.3}$$

for some $B_0 \in X_i$, we can recover D_1 from D_2. This proves the first equality.

To get the second equality, for each i, polynomials in X_i are mapped to a polynomial in X_j for some $1 \le j \le r$ via the map $B \mapsto B'$ except for at most one polynomial in X_i. So again from (2.3), we can change D_1 to $\mathcal{D}_M$ by elementary column operations. This completes the proof of the proposition. ∎

From Propositions 2.3 and 2.6, we have the following corollary which was already proved by Yin [Y, Main Theorem] in the global function field case.

COROLLARY 2.7. $[R^- : I^-] = \widetilde{h}_M^-$.

3. Exponent of the relative divisor class group Cl_M^-. Since G acts on the divisor class group Cl_M, we may view Cl_M as an R-module. It is well known (cf. [H, Theorem 1.1]) that the Stickelberger ideal I annihilates Cl_M. The relative divisor class group Cl_M^- is defined as $Cl_M^- = \{c \in Cl_M : c^{s(J)} = 1\}$.

For $\chi \in \widehat{G}$, let $e_\chi = (1/|G|)\sum_{A\in\mathbb{M}_M} \chi(A)\sigma_A^{-1} \in \mathbb{C}[G]$ be the idempotent element associated to χ. Recall $\eta = \sum_{A\in\mathbb{M}_M^+} \sigma_A^{-1}$. Then we have

$$\theta_M e_\chi = \eta e_\chi = h_\chi e_\chi$$

with $h_\chi = \sum_{A\in\mathbb{M}_M^+} \overline{\chi}(A)$. The following proposition is an analogue of Iwasawa's results [I, Theorems 7, 8]. The proof is almost immediate from the number field case, so we leave it to the reader.

PROPOSITION 3.1. *With the above notations, we have*:

(i) *Let t be the exponent of R^-/I^-, and let N denote the least positive integer such that N/h_χ is an algebraic integer for every odd character χ. Then N is a factor of $(q-1)t$ and t is a factor of $|G|N$.*

(ii) *The exponent of Cl_M^- is a factor of $|G|N$ and the exponent of $Cl_M^{(q-1)-s(J)}$ is a factor of $|G|N/(q-1)$.*

(iii) *Suppose that Cl_M^- is a cyclic group. Then h_M^- is a factor of $|G|N$.*

As t divides $|R^-/I^-| = \widetilde{h}_M^-$, it follows that if $(q-1, \widetilde{h}_M^-) = 1$, then t must be a factor of $|G|N/(q-1)$.

Let $C_0 = \{c \in Cl_M^- : c^{q-1} = 1\}$. Clearly C_0 is an R-submodule of Cl_M^-. As in [J, Theorem 1.4], we have

THEOREM 3.2. *Every cyclic R-submodule of Cl_M^-/C_0 is the homomorphic image of the quotient R^-/I^-. In particular, the exponent e of Cl_M^- divides $(q-1)t$, where t is the exponent of R^-/I^-.*

Proof. Let j be a generator of J as before, so $R^- = (1-j)R$. If $(1-j)f = (1-j)g$ with $f, g \in R$, then $(f-g) \in R^+ = s(J)R$. Thus $f - g = s(J)h$ for some $h \in R$ and $c^f = c^{g+s(J)h} = c^g$ for $c \in Cl_M^-$. For $c \in Cl_M^-$, we define a map $\tau_c : R^- \to Cl_M^-$ by $(1-j)f \mapsto c^f$. Then τ_c is a well-defined R-homomorphism of R^- onto c^R. For $s \in I^-$, we have $(q-1)s = ((q-1)-s(J))s = (1-j)hs$ for some $h \in R$. Since any element of the Stickelberger ideal annihilates the divisor class group, we have $\tau_c((q-1)s) = \tau_c((1-j)hs) = c^{hs} = 1$, i.e. $\tau_c(s)^{q-1} = 1$. Thus $I^- \subset \ker\tau_c$. Therefore $\tau_c : R^-/I^- \to Cl_M^-/C_0$ is a well-defined R-homomorphism and its image is the R-cyclic submodule c^R of Cl_M^-/C_0. This completes the proof of the theorem. ■

Let $h_M^- = \prod_i l_i^{e_i}$ be the prime factorization of h_M^-. The exponent e of Cl_M^- is divisible by $\prod_i l_i$. Suppose that l is a simple prime factor of the exponent t of R^-/I^- with $(l, q-1) = 1$. Then by Theorem 3.2, the l-Sylow subgroup of Cl_M^- is an elementary abelian group.

Let S_∞ be the set of infinite primes in K. Let $\mathcal{D}(S_\infty)^0$ be the group of degree zero divisors supported on S_∞ and $\mathcal{P}(S_\infty)$ be the group of principal divisors supported on S_∞. For the set S_∞^+ of infinite primes of K^+, $\mathcal{D}(S_\infty^+)^0$ and $\mathcal{P}(S_\infty^+)$ are defined similarly. Then we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty) & \longrightarrow & Cl_M & \longrightarrow & \widetilde{Cl}_M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{D}(S_\infty^+)^0/\mathcal{P}(S_\infty^+) & \longrightarrow & Cl_M^+ & \longrightarrow & \widetilde{Cl}_M^+ & \longrightarrow & 0, \end{array}$$

where each column is induced from the norm map N_{K/K^+}.

Let $(\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty))^-$ be the kernel of N_{K/K^+} in $\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty)$. From the above diagram, we have the exact sequence of R-modules

$$0 \to (\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty))^- \to Cl_M^- \to \widetilde{Cl}_M^- \to 0. \tag{3.1}$$

Thus we see that the results on Cl_M^- (Proposition 3.1, Theorem 3.2) also hold for the relative ideal class group $\widetilde{Cl}_M^-$.

As J is both the decomposition and the inertia group at ∞, $N_{K/K^+}(x) = (q-1)x$ for $x \in \mathcal{D}(S_\infty)$. Thus as an abelian group $(\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty))^-$ has the exponent dividing $q-1$. Since $\mathcal{D}(S_\infty)^0$ is a free abelian group of rank $r-1$, the order of $(\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty))^-$ divides $(q-1)^{r-1}$. But from $h_M^- = (q-1)^{r-1}\widetilde{h}_M^-$ and (3.1), we see $|(\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty))^-| = (q-1)^{r-1}$. Thus we have

PROPOSITION 3.3. $(\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty))^- \cong (\mathbb{Z}/(q-1))^{r-1}$. *In particular, if* $(\widetilde{h}_M^-, q-1) = 1$, *we have*

$$Cl_M^- \cong (\mathcal{D}(S_\infty)^0/\mathcal{P}(S_\infty))^- \oplus \widetilde{Cl}_M^- \cong (\mathbb{Z}/(q-1))^{r-1} \oplus \widetilde{Cl}_M^-.$$

Now we give some examples on the group structure of Cl_M^-. As the k-isomorphisms $T \mapsto T + \alpha$ with $\alpha \in \mathbb{F}_q^*$ send a monic irreducible polynomial to another monic irreducible polynomial, it suffices to consider only the polynomials up to these isomorphisms. We compute the invariants of R^-/I^-, i.e., the invariants of the Dem'yanenko matrix $\mathcal{D}_M$ using MAPLE. The computation of invariants from the matrix becomes difficult as the size of the matrix becomes larger.

EXAMPLE 1. Suppose $M = P$ with $\deg P = 1$. Then $R^- = I^-$ by Lemmas 2.1, 2.2 and so Cl_M^- is trivial.

EXAMPLE 2. We give examples with $q = 3$, $M = P$, $\deg P \leq 4$. A simple calculation shows that $\widetilde{h}_M^-$ is prime to $q-1$ if $\deg P \leq 4$. Thus, by Proposition 3.3, it suffices to determine the structure of $\widetilde{Cl}_M^-$.

For $\deg P = 2$, T^2+1 is the only nonisomorphic monic irreducible polynomial and $\widetilde{h}^-_{T^2+1} = 1$. Thus $\widetilde{Cl}^-_M$ is trivial and $Cl^-_M \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

For $\deg P = 3, 4$, there are 4 and 6 nonisomorphic monic irreducible polynomials, respectively. Tables 1 and 2 show the order and the structure of the relative ideal class group for each polynomial. When $\widetilde{h}^-_P$ is square-free, obviously $\widetilde{Cl}^-_P$ is cyclic. When $\widetilde{h}^-_P$ is not square-free, we compute the invariants of R^-/I^-. If the exponent of R^-/I^- is square-free, then each l-Sylow subgroup of $\widetilde{Cl}^-_P$ is an elementary abelian l-group. We label such cases "elementary" in Tables 1 and 2. If the exponent of R^-/I^- has a nonsimple prime factor l, we cannot determine the l-Sylow subgroup of $\widetilde{Cl}^-_P$ from our results. In this case we only write the nonsimple factors of the exponent of R^-/I^- in Tables 1 and 2.

Table 1. $p = 3, \deg P = 3$

$P(T)$	$\widetilde{h}^-_M$	$\widetilde{Cl}^-_M$
T^3+T^2+2	$5 \cdot 79$	cyclic
T^3+2T^2+1	$3 \cdot 131$	cyclic
T^3+2T+2	$3^3 \cdot 7$	elementary
T^3+2T+1	3^6	3^2

Table 2. $p = 3, \deg P = 4$

$P(T)$	$\widetilde{h}^-_M$	$\widetilde{Cl}^-_M$
T^4+T+2	$241 \cdot 641 \cdot 881 \cdot 532611841$	cyclic
T^4+2T+2	$17 \cdot 97 \cdot 63648628175761$	cyclic
T^4+T^2+2	$241 \cdot 3329 \cdot 65521 \cdot 1322641$	cyclic
T^4+2T^2+2	$17^3 \cdot 12046669609441$	elementary
T^4+T^2+T+1	$17^2 \cdot 337 \cdot 853111437361$	elementary
T^4+T^2+2T+1	$17^2 \cdot 13921 \cdot 18743655761$	17^2

EXAMPLE 3. Let $q = 7$ and $M = T^2$. We have $\widetilde{h}^-_M = 2^3 \cdot 13^2 \cdot 118147$ and the exponent of R^-/I^- is $2 \cdot 13 \cdot 118147$. As $(\widetilde{h}^-_M, q-1) = 2$, we only see that the l-Sylow subgroup of Cl^-_M is an elementary abelian l-group for $l \neq 2$ and the 2-factor of the exponent of Cl^-_M is 2 or 4 from Theorem 3.2.

4. The signs of cyclotomic units. Recall that for $0 \neq A \in \mathbb{A}$, $\operatorname{sgn}(A)$ denotes the leading coefficient of A. This function can be extended to a sign function (also denoted by "sgn") on k_∞, i.e., $\operatorname{sgn} : k^*_\infty \to \mathbb{F}^*_q$ which is the identity on $\mathbb{F}^*_q$ and trivial on $U^{(1)}_\infty$. Here $U^{(1)}_\infty$ is the subgroup of 1-units of k^*_∞.

Let $\mathfrak{P}$ be an infinite prime of K and $\mathfrak{p}$ be the infinite prime of K^+ lying below $\mathfrak{P}$. From [GR, Proposition 1.10], there exists a primitive M-torsion point λ such that $\mathrm{ord}_{\mathfrak{P}}(\lambda) = (d-1)(q-1)-1$, where $d = \deg M$. As $\mathfrak{p}$ is totally ramified in K, we also have $\mathrm{ord}_{\mathfrak{p}}(\lambda^{q-1}) = (d-1)(q-1)-1$. Since the completion $(K^+)_{\mathfrak{p}}$ of K^+ at $\mathfrak{p}$ is isomorphic to k_∞, we regard K^+ as a subfield of k_∞ under this isomorphism.

Proposition 4.1. $\mathrm{sgn}(\lambda^A/\lambda) = \mathrm{sgn}_M(A)$ *for* $0 \neq A \in \mathbb{A}, (A, M) = 1$.

Proof. Since $\lambda^A = \lambda^{\overline{A}}$ and $\mathrm{sgn}_M(A) = \mathrm{sgn}_M(\overline{A})$, we may assume $A \in \mathbb{M}_M$ with $\deg A = d_0 \leq d-1$. Then λ^A/λ can be written as $\lambda^A/\lambda = \sum_{i=0}^{d_0} c(A,i)\lambda^{q^i-1}$, where $c(A,i)$ is a polynomial of degree $(d_0-i)q^i$ and $c(A,0) = A, c(A,d_0) = \mathrm{sgn}(A)$. For $0 \leq i \leq d_0$, we have

$$\begin{aligned}\mathrm{ord}_\infty&(c(A,i)\lambda^{q^i-1})\\ &= -(d_0-i)q^i + \frac{q^i-1}{q-1}((d-1)(q-1)-1)\\ &= \frac{1}{q-1}\{q^i((q-1)(i-d_0+d-1)-1) - ((d-1)(q-1)-1)\}.\end{aligned}$$

As $(q-1)(i-d_0+d-1)-1 \geq 0$ except for $d_0 = d-1$ and $i = 0$, $\mathrm{ord}_\infty(c(A,i)\lambda^{q^i-1})$ is an increasing function on i. Thus $\lambda^A/\lambda = xA$ with $x = 1+\sum_{i=1}^{d_0} c(A,i)\lambda^{q^i-1}/A \in U_\infty^{(1)}$. Therefore $\mathrm{sgn}(\lambda^A/\lambda) = \mathrm{sgn}(x)\,\mathrm{sgn}(A) = \mathrm{sgn}(A)$. ∎

Corollary 4.2. *For* $A, B \in \mathbb{M}_M^+$, $\mathrm{sgn}(\sigma_B(\lambda^A/\lambda)) = \mathrm{sgn}_M(AB)$.

For a fixed generator α in $\mathbb{F}_q^*$, we define $\overline{\mathrm{sgn}}_\alpha : k_\infty^* \to \mathbb{Z}/(q-1)$ as $\mathrm{sgn}(x) = \alpha^{\overline{\mathrm{sgn}}_\alpha(x)}$ for $x \in k_\infty^*$. An element x of K^+ is called *totally positive* if $\overline{\mathrm{sgn}}_\alpha(\sigma(x)) = 0$ for any $\sigma \in G_M^+$. Write $\mathbb{M}_M^+ = \{A_1, \ldots, A_r\}$ with $A_1 = 1$ and $\sigma_i = \sigma_{A_i}$. Let E be the group of units in $\mathcal{O}_M$ and E_{cyc} be the group of cyclotomic units [GR, Section 4]. Then

$$E = \mathbb{F}_q^* \times \prod_{i=2}^{r} \langle \varepsilon_i \rangle \quad \text{and} \quad E_{\mathrm{cyc}} = \mathbb{F}_q^* \times \prod_{i=2}^{r} \langle \xi_i \rangle,$$

where $\{\varepsilon_i\}_i$ is a system of fundamental units for E and $\xi_i = \lambda^{A_i}/\lambda$. Let $\xi_1 = \varepsilon_1 = \alpha$. For $i \geq 2$, we can write ξ_i as $\xi_i = \alpha^{n_i}\prod \varepsilon_j^{c_{ij}}$ with $n_i, c_{ij} \in \mathbb{Z}$. Let $A = (c_{ij})_{i,j\geq 2}^t$. Then

$$(\xi_1, \ldots, \xi_r) = (\varepsilon_1, \ldots, \varepsilon_r) \cdot \begin{pmatrix} 1 & * \\ 0 & A \end{pmatrix}$$

and so

$$(\mathrm{sgn}(\sigma_k(\xi_i)))_{k,i} = (\mathrm{sgn}(\sigma_k(\varepsilon_i)))_{k,i} \cdot \begin{pmatrix} 1 & * \\ 0 & A \end{pmatrix}. \tag{4.1}$$

Note that the matrix A is uniquely determined modulo $q-1$ in (4.1).

Now assume $q=3$. Note that $\overline{\mathrm{sgn}}_\alpha(\sigma_k(\xi_i))$ becomes $\langle A_i A_k\rangle + 1$ if $i \neq 1$ and 1 if $i=1$. From (4.1), we have

$$(\overline{\mathrm{sgn}}_\alpha(\sigma_k(\xi_i)))_{k,i} = (\overline{\mathrm{sgn}}_\alpha(\sigma_k(\varepsilon_i)))_{k,i} \cdot \begin{pmatrix} 1 & * \\ 0 & A \end{pmatrix} \quad \text{in } \mathbb{F}_2. \tag{4.2}$$

LEMMA 4.3. *Let* $\mathcal{E}_M = (\overline{\mathrm{sgn}}_\alpha(\sigma_k(\xi_i)))_{k,i}$. *Then* $|\det \mathcal{E}_M| \equiv \widetilde{h}_M^- \bmod 2$.

Proof. Since α has order 2, we have $\mathcal{D}_M = (\langle A_i A_k\rangle)_{i,k}$. By adding the first column of $\mathcal{D}_M$ to the other columns, we change $\mathcal{D}_M$ into $\mathcal{E}_M$ in $\mathbb{F}_2$. Now the lemma follows from Proposition 2.6. ∎

Let E^+ (resp. E^+_{cyc}) denote the subgroup of totally positive units in E (resp. E_{cyc}). Then, as in [S, Theorem 1], we get the following theorem.

THEOREM 4.4. *The following are equivalent*:

(i) $2 \mid \widetilde{h}_M^-$.
(ii) $E^+_{\mathrm{cyc}} \neq E^2_{\mathrm{cyc}}$.
(iii) $2 \mid \widetilde{h}_M^+$ or $E^+ \neq E^2$.

Proof. Consider a homomorphism

$$\phi : E \to \mathbb{F}_2^r, \qquad x \mapsto (\overline{\mathrm{sgn}}_\alpha(\sigma_1(x)), \ldots, \overline{\mathrm{sgn}}_\alpha(\sigma_r(x))).$$

Since E^+ (resp. E^+_{cyc}) is the kernel of ϕ in E (resp. E_{cyc}), we have $|E/E^+| = 2^{d_1}$ and $|E_{\mathrm{cyc}}/E^+_{\mathrm{cyc}}| = 2^{d_2}$, where $d_1 = \mathrm{rank}(\overline{\mathrm{sgn}}_\alpha(\sigma_k(\varepsilon_i)))_{k,i}$ and $d_2 = \mathrm{rank}(\overline{\mathrm{sgn}}_\alpha(\sigma_k(\xi_i)))_{k,i}$. Now the result follows from (4.2), Lemma 4.3 and the fact that $|\det A| = \widetilde{h}_M^+$ (cf. [GR, Main Theorem]). ∎

References

[BK] S. H. Bae and P.-L. Kang, *Class numbers of cyclotomic function fields*, Acta Arith. 102 (2002), 251–259.

[GR] S. Galovich and M. Rosen, *Units and class groups in cyclotomic function fields*, J. Number Theory 14 (1982), 156–184.

[H] D. Hayes, *Stickelberger elements in function fields*, Compositio Math. 55 (1985), 209–239.

[Ha] F. Hazama, *Demjanenko matrix*, *class numbers*, *and Hodge group*, J. Number Theory 34 (1990), 174–177.

[I] K. Iwasawa, *A note on ideal class groups*, Nagoya Math. J. 27 (1966), 239–247.

[J] V. Jha, *A free basis of the Stickelberger ideal of some imaginary cyclic number fields and application to the structure of the class groups*, CICMA Report 1994-06.

[JA] H. Jung and J. Ahn, *Demjanenko matrix and recursion formula for relative class number over function fields*, J. Number Theory, to appear.

[R] M. Rosen, *A note on the relative class number in function fields*, Proc. Amer. Math. Soc. 125 (1997), 1299–1303.

[S] W. Schwarz, *Demjanenko matrix and 2-divisibility of class numbers*, Arch. Math. (Basel) 60 (1993), 154–156.

[W] L. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

[Y] L. Yin, *Stickelberger ideals and relative class numbers in function fields*, J. Number Theory 81 (2000), 162–169.

Department of Mathematics
KAIST
Daejon, South Korea 305-701
E-mail: hyjung@mathx.kaist.ac.kr
jaehyun@mathx.kaist.ac.kr

Received on 17.9.2001
and in revised form on 13.5.2002 (4111)